PROPROSTA DE MITIGAÇÃO A ATAQUES PHISHING EM UMA EMPRESA DO RAMO AUTOMOTIVO

PHISHING ATTACK MITIGATION PROPOSAL IN AN AUTOMOTIVE COMPANY

Carlos Alexandre Rodrigues Bernadino
Fatec Santana de Parnaíba
calexandre49@gmail.com

Renan Contidorio Magagnini
Fatec Santana de Parnaíba
magagninirenan@gmail.com

Luiz Rodrigo Gomes de Oliveira
Fatec Santana de Parnaíba
luiz.oliveira173@fatec.sp.gov.br

Resumo

O advento do uso massivo da internet e o aumento do trabalho remoto, com a utilização de dispositivos digitais no compartilhamento de informações, tornou necessário para as empresas terem uma equipe de colaboradores consciente e preparada para a crescente demanda de ataques de engenharia social para a proteção de seus dados confidenciais, sendo um dos principais problemas enfrentados o ataque de *phishing*. Uma das ferramentas mais utilizadas pelos atacantes para conseguir enganar equipes de trabalhadores e obter êxito dentro desse contexto, gerando grandes prejuízos e danos a setores ou a empresa como um todo. Esse artigo analisa os impactos de um ataque de *phishing* dentro de um ambiente corporativo, com o objetivo de identificar falhas, oportunidades de melhorias e apresentar uma proposta abrangente para mitigação de possíveis ataques e prevenção aos seus danos. A pesquisa utiliza a metodologia de estudo de caso único, com coleta de dados por meio de questionário e testes práticos de ataques. Os Resultados são a contribuição para a prática, proporcionando que gestores de TI possam se beneficiar com a proposta e sugestões desta pesquisa, já a contribuição para a academia é acrescentar em pesquisas futuras que envolvam formas de contenção a ataques relacionados a engenharia social.

Palavras-chave: *Phishing*, ataque, mitigação, setor automotivo, engenharia social, ciberataque.

Abstract

The advent of massive use of the internet and the increase in remote work, with the use of digital devices to share information, has made it necessary for companies to have a team of employees aware and prepared for the growing demand for social engineering attacks to protect of confidential data. One of the main problems faced is phishing attacks. One of the tools most used by attackers to deceive teams of workers and be successful within this context, causing great losses and damage to sectors or the company as a whole. This article analyzes the impacts of a phishing attack within a corporate environment, with the aim of identifying and presenting a comprehensive proposal for mitigating damage or preventing threats. The research used a single case study methodology, with data collection through interviews and practical attack tests. The Results are the contribution to practice, allowing IT managers to benefit from the proposal and suggestions of this research, while the contribution to academia includes adding to future research involving forms of containment of attacks related to social engineering.

Keywords*: Phishing, attack, mitigation, automotive sector, social engineering, cyberattack.*

1. Introdução

A crescente digitalização dos processos corporativos que ocorreram de forma acelerada e forçada com a chegada da pandemia do covid-19, muitas empresas tiveram que disponibilizar recursos para que seus colaboradores pudessem trabalhar, mas nem todas conseguiram disponibilizar as ferramentas, treinamentos e muitas vezes até times de suporte adequados que colaborassem com a redução de ataques que se está suscetível neste tipo de ambiente (PEREIRA; NEVES, 2021)

Em meio a tantos tipos de ataques, os que utilizam engenharia social vêm ganhando notoriedade pela facilidade de se infiltrar em ambientes corporativos através do usuário, afim de extrair dados sensíveis que possam acarretar prejuízos financeiros e de imagem da empresa, muitas vezes irreversíveis. De todos os 23.619 incidentes cibernéticos analisados em 81 empresas, cerca de 15% eram relacionados a ataques de *phishing* em 2020 (VERIZON, 2020).

Desta forma, é necessário estabelecer métodos de mitigação para reduzir este tipo de ataque em ambiente corporativo e reverter a ideia de usuário como “elo mais fraco” dentro da hierarquia de segurança da informação (FONSECA, 2017). Tais métodos envolvem a utilização de treinamento adequado com a utilização de linguagem inteligível para o público leigo e a capacitação humana através de processos, ferramentas e normas que contribuam com o aumento de conhecimento, atenção e senso de impacto, reduzindo o número de incidentes de *phishing*.

Em 2023 foi evidente que a indústria manufatureira principalmente em setores como indústrias de peças, automotiva, e de tecnologia tem sido extremamente almejado por tais ataques, principalmente por conta do valor de uma grande massa de dados envolvidos e informações privilegiadas de uma grande rede de relacionamento entre essas empresas (VERIZON, 2023). Isso demonstra a importância de uma empresa do setor automotivo se preparar cada vez mais para prevenção de tais ataques utilizando-se de diferentes métodos.

Diante deste contexto, o presente trabalho possui como questão de pesquisa: “Como uma empresa do setor automotivo pode mitigar ataques *phishing*?”. Os objetivos são: (1) Identificar e apresentar uma proposta abrangente para mitigação dos danos ou prevenção contra as ameaças (2) Analisar os impactos de um ataque de *phishing* dentro de uma empresa do setor automotivo.

2. Referencial Teórico

Nesta seção serão apresentados os principais termos e tecnologias que serão utilizadas para alcançar os objetivos propostos na área de segurança da informação, com foco na engenharia social e *phishing*.

2.1. Segurança da Informação

Quando abordado o tema da segurança da informação, estamos nos referindo a um conceito abrangente, visto que vivemos em um mundo interconectado, com a utilização de plataformas *Cloud* como *Amazon Web Services* (AWS), permitindo a criação de instâncias com sistemas operacionais diversos como Ubuntu e serviços *Web* como Apache pelo *Elastic Compute Cloud* (EC2), permitindo que pequenas organizações possam obter sua própria infraestrutura com equipes de TI reduzidas (SILVA, 2023)

Com isso devem ser protegidas as informações compartilhadas garantindo os seus pilares principais de confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade. Em termos simples, a segurança busca evitar que pessoas não autorizadas acessem as informações utilizando dispositivos de segurança pré-definidos para monitorar o tráfego na rede como *Firewall*, *Instrusion Detection System* (IDS), *Intrusion Prevention System* (IPS) gerando alertas e ações de contramedidas, Proxy para filtro de páginas *web*, garantindo que as informações estejam em um local apropriado e disponíveis (FONTES, 2017).

Confidencialidade tem por objetivo preservar restrições autorizadas no acesso e na divulgação de informações. É implementada através de mecanismos de segurança que distinguem usuários autorizados de usuários não autorizados como o *Active Directory* (AD), de forma a garantir que as informações de um ambiente privado não sejam acessadas por terceiros ou partes indevidas (OLIVEIRA TEODORO; CISA, 2020).

A integridade concentra-se em garantir que os dados permaneçam precisos e inalterados, a menos que tais mudanças sejam autorizadas. Alguns mecanismos como políticas e modelos de autorização tem um papel de extrema importância na configuração e aplicação de regras de acesso dentro de sistemas (MOHAMED et al., 2022).

A disponibilidade assegura que os dados e informações estejam sempre acessíveis e disponíveis aos usuários autorizados de um sistema quando se fizer necessário. O princípio trata sobre a importância de manter a informação e serviços prontamente disponível para atender aos processos e objetivos de uma organização. A ferramenta Zabbix, por exemplo, permite uma visão ampla da disponibilidade da organização, utilizando recursos para monitorar, coletar e exibir métricas da infraestrutura de TI, rede, servidores, máquinas virtuais e serviços em nuvem (FREUND et al., 2019).

A autenticidade tem o objetivo de validar se uma pessoa é realmente quem diz ser. A autenticação é necessária para controlar o acesso e auditar sistemas e informações sensíveis, uma ferramenta criada para garantir a autenticidade das operações online são os certificados digitais emitidos por autoridades certificadas como a Let's Encrypt e outras. (SOUZA, 2022).

Por fim, o não repúdio, ou irretratabilidade. Ele garante que o autor não negue ter realizado determinada ação. Isso é importante em ambientes em que transações, visando que as partes envolvidas não possam dizer que não realizaram uma ação (GONÇALVES; OGAWA; LIMA, 2022).

2.2. Fator humano

O fator humano é considerado o elo mais fraco em um sistema de informação, é considerado a maior porta de acesso aos dados tanto do próprio usuário quanto para as empresas. Os engenheiros sociais utilizam suas habilidades de persuasão para conseguir informações, explorando as emoções humanas como a ingenuidade, medo, confiança e todas essas características emocionais. Por conta do uso dessas técnicas de manipulação a fragilidade humana está diretamente ligada ao sucesso de ataques (FONSECA, 2017).

A engenharia social é a ciência do uso da interação social para manipular pessoas, por meio de técnicas e ferramentas com objetivo de obter informações, ou qualquer vantagem sobre uma pessoa ou empresa, visando as vulnerabilidades do ambiente. O uso de técnicas de manipulação para persuasão, muitas vezes aproveitando da ingenuidade ou confiança do usuário, para obter acesso não autorizado a informações sigilosas (DIAS, 2021).

2.3. Phishing

Phishing é a técnica que consiste em um ataque com objetivo de roubar informações privadas, como por exemplo: login e senha, dados bancários, informações sensíveis etc. (GONÇALVES; OGAWA; LIMA, 2022). A técnica também tem o objetivo de instalar *software* maliciosos no equipamento alvo se passando por uma entidade confiável. O principal meio utilizado por esse ataque são *e-mails*, *links* que redirecionam para um *site* de *phishing* onde possui aparência oficial, ou anexo de conteúdo malicioso (PEREIRA; NEVES, 2021), possíveis golpes por meio de redirecionamentos, geralmente chamados de spoofing e envenenamento são tipos de ataques virtuais que exploram as vulnerabilidades de Sistema de Nomes de Domínio (DNS) para desviar o tráfego de servidores legítimos para servidores falsos, encontrado em URLs enviados por *e-mails* de *spam* (KASPERSKY, 2024).

Segundo dados de 2023 pela empresa VERIZON as três principais formas pelas quais os invasores acessam uma organização são credenciais roubadas, *phishing* e exploração de vulnerabilidades, quando obtém acesso adicionam *backdoors* para manter esse acesso. O *phishing* fornece apenas mais um meio de entrada, seja para obter um conjunto de credenciais utilizáveis ou para infectar um sistema com *malware* amplamente distribuído por *e-mail*, e muitas vezes enviados na forma de documentos Microsoft Office com o intuito de influenciar ao usuário executá-lo (VERIZON, 2023).

Em um estudo detalhado é possível identificar que os ataques geralmente iniciam com a coleta de informações sobre o alvo e escolha do método de ataque. Em exemplos reais os atacantes utilizam de *e-mails* que induzem palavras de urgência, endereços de remetente que se assemelham ao original, e principalmente *links* falsos que ao serem clicados conduzem o ataque geralmente com vírus ou *malwares*. Fatores como a abordagem de urgência e endereços de *e-mail* desconhecidos são importantes sinais de alerta (ALKHALIL *et al*., 2021).

Para avaliar as medidas de mitigação de *phishing* é fundamental analisar a eficácia das estratégias *anti-phishing*, que abordam uma variedade de medidas preventivas como utilização de antivírus e outras. Sendo necessária a educação contínua dos usuários, uso de *frameworks* e *software* para simulação de testes como o *Gophish* podendo assim distinguir o desempenho das contramedidas contra as ameaças de *phishing*, e compreender a capacidade dos usuários de detectar tentativas de *phishing* (LIMA, 2022).

2.4. Setor Automotivo

A indústria ou setor automotivo engloba uma ampla variedade de empresas e organizações envolvidas no design, desenvolvimento, fabricação, *marketing* e venda de veículos motorizados (MASOUMI; KAZEMI; ABDUL-RASHID, 2019). É um dos setores econômicos que se destacam no volume de vendas e empregam uma vasta força de trabalho no mundo todo, com operações que vão desde a produção de peças automotivas até a montagem final dos veículos (CASOTTI; GOLDENSTEIN, 2008).

Os ataques de *phishing* na indústria automotiva não apenas comprometem informações individuais, mas também podem interromper as operações de produção. Com uma cadeia de suprimentos global e muitas vezes conectada, um ataque bem-sucedido em um ponto pode se expandir ao longo de toda a rede. Além disso, esses ataques visam frequentemente roubar propriedade intelectual ou comprometer os sistemas de produção automotiva, o que pode ocasionar em perdas financeiras significativas (DAVIES, 2023).

Segundo um relatório da VERIZON (2023), a indústria manufatureira que engloba setores como a construção civil, indústrias de peças para aeronaves, automóveis, tecnologia, alimentícia, entre outros, é um dos mais visados por tais ataques, devido à sua ampla rede de fornecedores e à quantidade de dados sensíveis envolvidos (VERIZON, 2023). Com isso, se faz cada vez mais necessário com que as empresas desse ramo estejam constantemente atualizadas e atentas para que possam mitigar ao máximo sofrer esses tipos de ataques através do *phishing* que tem sido uma das técnicas preferidas dos atacantes e que pode comprometer toda a empresa e em alguns casos todo o setor (ALKHALIL *et al*., 2021).

3. Metodologia

A metodologia a ser adotada a esta pesquisa pertence a abordagem qualitativa, por meio do Estudo de Caso Único (YIN, 2014) em um Ambiente Industrial do Segmento Automotivo, onde os métodos e ferramentas para análise e identificação de ataques de *phishing* foram aplicação de formulário para identificar o nível de conhecimento, coleta de informações e testes práticos. Será realizada a interpretação dos resultados e propostas para mitigação de ataques no ambiente industrial automotivo, bem como realizar estudo do comportamento humano.

3.1. Processo Metodológico

Essa pesquisa está dividida por 7 etapas, descritas abaixo:

Passo 1: Criar o Questionário. Foi criado um questionário para ser aplicado com um intuito de coletar dados sobre a eficiência da empresa com ataques *phishing* e os pontos aos quais podem ser determinantes para uma possível falha, que deverá ser encaminhado a gerência de TI

Passo 2: Aplicar o Qustionário. Foi aplicado o questionário (Apêndice A) ao gerente de TI em 18/04/2024.

Passo 3: Identificar a Arquitetura de TI. Identificação dos processos e ferramentas de TI que a empresa utiliza por meio de sua arquitetura para avaliar onde estão os possíveis pontos de vulnerabilidade ou alvos de ataques.

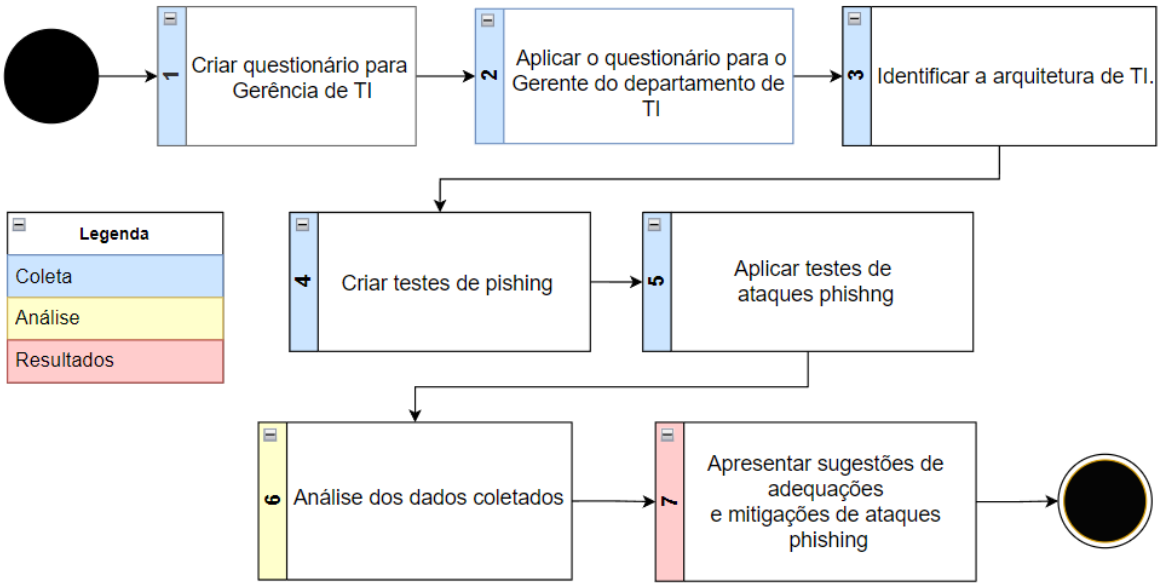
Passo 4: Criar testes de *phishing*. Testes criados baseando-se na arquitetura e na principal técnica utilizada pelos atacantes de *phishing*: Engenharia social.

Passo 5: Aplicar testes de *phishing*. Testes aplicados nos dias 29 e 31 de maio com o aval da equipe de TI, no qual gerou um relatório com resultado da exposição da organização ao *phishing*.

Passo 6: Análise dos dados coletados. Análise dos dados coletados por meio de questionário, elaboração da arquitetura e aplicação dos testes de *phishing* para que possam ser levantados as principais vulnerabilidades relacionadas a ataques *phishing*

Passo 7: Apresentar sugestões de adequações e mitigações de ataques *phishing*. As sugestões serão baseadas na análise dos dados coletados e nas vulnerabilidades identificadas.

Figura 1 – Processo Metodológico



Fonte: Elaborado pelos autores, 2024

3.2. Objeto de Estudo

A Empresa-Alpha é uma corporação que possui matriz no estado de São Paulo há mais de 5 anos. Possui grandes clientes nacionais e internacionais na fabricação de peças para distribuição e controle de energia elétrica em veículos automotores contando com aproximadamente 70 colaboradores.

A empresa também atua nas áreas de usinagem, tornearia, solda, e fabricações de outros produtos de metal.

3.3. Criação do questionário

O questionário foi criado com o objetivo de obter informações e coletar dados importantes relacionados a cultura, ferramentas e processos que estão relacionados a empresa no contexto de maturidade na prevenção a ataques *phishing*. Esses dados serão utilizados para que sejam criados os testes e para a elaboração da proposta de mitigação advindo da sugestão de melhorias.

Foram criadas 10 questões baseando-se nos tópicos e afirmações consideradas importantes para elucidar os pontos positivos e possíveis falhas no tratamento da empresa em relação a segurança da informação e ataques de *phishing*.

O único respondente será o Gerente de TI da Empresa-Alpha

Tabela 1 – Relação de maturidade da Empresa-Alpha

Base Teórica	Questões
O fator humano é considerado o elo mais fraco onde é a maior porta de acesso aos dados tanto do próprio usuário como para empresas. Fonseca (2017) cita que os engenheiros sociais utilizam suas habilidades de persuasão para conseguir informações, explorando as emoções humanas como a ingenuidade, medo, confiança e todas essas características emocionais.	Quais medidas proativas são implementadas para educar os funcionários sobre os riscos do *phishing*? Como incentivar uma cultura de segurança cibernética em toda a organização, onde todos os funcionários se sintam responsáveis pela prevenção de ataques de *phishing*?
Segundo dados de 2023 pela empresa VERIZON as três principais formas pelas quais os invasores acessam uma organização são credenciais roubadas, *phishing* e exploração de vulnerabilidades, quando obtém acesso adicionam *backdoors* para manter esse acesso. O *phishing* fornece apenas mais um meio de entrada, seja para obter um conjunto de credenciais utilizáveis ou para infectar um sistema com *malware* amplamente distribuído por *e-mail*, e muitas vezes enviados na forma de documentos Microsoft Office com o intuito de influenciar ao usuário executá-lo.	Quais tecnologias de segurança adicionais são adotadas para detectar e bloquear melhor os ataques de *phishing*?

Base Teórica	Questões
O fator humano é considerado o elo mais fraco onde é a maior porta de acesso aos dados tanto do próprio usuário como para empresas. Os engenheiros sociais utilizam suas habilidades de persuasão para conseguir informações, explorando as emoções humanas como a ingenuidade, medo, confiança e todas essas características emocionais. Por conta do uso dessas técnicas de manipulação a fragilidade do fator está diretamente ligada ao sucesso de ataques (FONSECA, 2017).	Como é possível implementar treinamentos regulares de conscientização sobre segurança cibernética para garantir que os funcionários estejam atualizados sobre as últimas táticas de *phishing*?
Phishing é a técnica que consiste em um ataque com objetivo de roubar informações privadas, como por exemplo: login e senha, dados bancários, informações sensíveis etc. A técnica também tem o objetivo de instalar *software* maliciosos no equipamento alvo se passando por uma entidade confiável. O principal meio utilizado por esse ataque são *e-mails*, *links* que redirecionam para um *site* de *phishing* onde possui aparência oficial, ou anexo de conteúdo malicioso (DE LUCAS BASTOS; NEVES; OTHERS, 2021)	Como a empresa pode fortalecer a política de segurança de *e-mail* para filtrar e identificar melhor *e-mails* de *phishing*? Quais são as práticas adotadas pela empresa para verificar a autenticidade de *e-mails* suspeito antes de clicar em *links* ou fornecer informações confidenciais?
A autenticidade tem o objetivo de validar de que uma pessoa é realmente quem diz ser. A autenticação é necessária para controlar o acesso a auditar sistemas e informações sensíveis (DE SOUZA, 2022).	Como foi implantada as políticas de acesso e permissões que limitem o acesso a informações confidenciais, mesmo em caso de comprometimento de credenciais?
Em um estudo detalhado é possível identificar que os ataques geralmente iniciam com a coleta de informações sobre o alvo e escolha de método de ataque. Em exemplos reais os atacantes utilizam de *e-mails* que induzem palavras de urgência, endereços de remetente que se assemelham ao original, e principalmente *links* falsos que ao serem clicados conduzem o ataque geralmente com vírus ou *malwares*. Fatores como a abordagem de urgência e endereços de *e-mail* desconhecidos são importantes sinais de alerta (ALKHALIL et al., 2021).	Quais são os sinais de alerta precoce que devem estar atentos para identificar possíveis ataques de *phishing* direcionadas à empresa?
Phishing é a técnica que consiste em um ataque com objetivo de roubar informações privadas, como por exemplo: login e senha, dados bancários, informações sensíveis etc. A técnica também tem o objetivo de instalar *software* maliciosos no equipamento alvo se passando por uma entidade confiável. O principal meio utilizado por esse ataque são *e-mails*, *links* que redirecionam para um *site* de *phishing* onde possui aparência oficial, ou anexo de conteúdo malicioso (DE LUCAS BASTOS; NEVES; OTHERS, 2021)	Quais são os riscos específicos de *phishing* associados a fornecedores e parceiros externos e como podem mitigá-los?
Para avaliar as medidas de mitigação de *phishing* é fundamental analisar a eficácia das estratégias *anti-phishing*, que abordam uma variedade de medidas preventivas. Sendo necessário a educação contínua dos usuários, uso de *frameworks* e *software* para distinguir o desempenho das contramedidas contra as ameaças de *phishing*, e compreender a capacidade dos usuários de detectar tentativas de *phishing* (LIMA, 2022).	Como vocês avaliam regularmente a eficácia das medidas de mitigação de *phishing* e fazer ajustes conforme necessário?

4. Avaliação dos resultados

Os resultados do estudo foram obtidos a partir de um questionário respondido pela associação, e da análise da arquitetura, cultura e testes de ataques *phishing* realizados na empresa Alpha.

4.1. Análise do questionário aplicado a Gerência de TI

Por meio do questionário foi possível identificar que a empresa fornece recomendações básicas a seus colaboradores sobre prevenção a ataques de *phishing* como: atenção ao endereço do remetente que enviou a mensagem, não responder *e-mails* que estão fora do escopo de trabalho além de avaliar *links* e anexos, conforme citado pelo respondente.

Desta forma, o ponto de atenção quando se trata de *e-mails* internos e enviados por clientes que mesmo sendo considerados rementes confiáveis podem estar sendo manipulados por um terceiro ou haver má intenção por parte de funcionários.

A empresa possui ferramentas de *firewall* e filtros de *spam* mas não possui monitoramento de rede ativo relacionados à segurança como ferramentas IDS ou IPS, somente a ferramenta Zabbix para a elaboração de métricas, também não possui um *software* especializado para análise de *e-mails* ou conteúdos maliciosos na rede, conforme também mencionado pelo gerente de TI, o que pode acarretar em incidentes cibernéticos se o usuário for enganado ou manipulado através de *e-mails*, *sites* não filtrados, *links* ou arquivos maliciosos.

Também não são realizados testes e treinamentos frequentes relacionados ao tema, mas foi uma das práticas em que a gerência da empresa considerou como um fator determinante para a melhoria dos processos e de cultura relacionados à segurança da informação. Foi informado que poderiam ser realizados treinamentos e instruções semanais para conscientização e melhoria de conhecimento dos colaboradores.

A validação do ambiente é realizada diariamente pelos colaboradores da área de TI através das métricas geradas pela ferramenta passiva de monitoramento de rede (Zabbix)

4.2. Análise da arquitetura de TI da empresa

Antes da pesquisa a empresa ainda não possuía um desenho de arquitetura de TI e foi necessário trabalhar junto a gerência da área para que fosse realizado o desenho em conjunto que se encontra no apêndice B.

A empresa possui instalações que estão presentes em dois pisos, com toda a conexão de rede realizada via barramento e contendo um servidor que é utilizado para registro de usuário e ativos da rede com o *Active Directory* e também como servidor de *e-mail*.

4.3. Aplicação dos testes de ataques *Phishing*

Os testes de *Phishing* foram elaborados baseando-se na arquitetura e em todas as áreas em que foi possível identificar a utilização de internet, *e-mail* e documentos presentes na rede. Foram elaborados os testes personalizados para todas as áreas da organização exceto produção (corte de jato e montagem de peças).

A ferramenta utilizada para elaboração dos *e-mails* e coleta de dados foi a GoPhish que é um *framework* de simulação de ataques *phishing* de código aberto projetada para ajudar as organizações a treinarem seus funcionários contra-ataques *phishing*, ela permite a criação de modelos de *e-mail* e a elaboração de dashboards com os resultados dos testes, exibindo os funcionários que abriram *e-mails*, clicaram em *links*, arquivos maliciosos e inseriram informações de credenciais da organização.

Utilizamos de uma instancia EC2 na plataforma AWS com sistema operacional Ubuntu versão 22.04 para instalação do *framework* Gophish, feito aquisição de um domínio público, instalação do servidor web Apache2 para emissão de certificado digital pela *Let's Encrypt*, configuração e apontamento de DNS com intuito de eliminar suspeitas e burlar ferramentas de segurança como *Proxy*/*Firewall*. Criação de *e-mail* utilizando o domínio público para transparecer segurança aos alvos a serem testados.

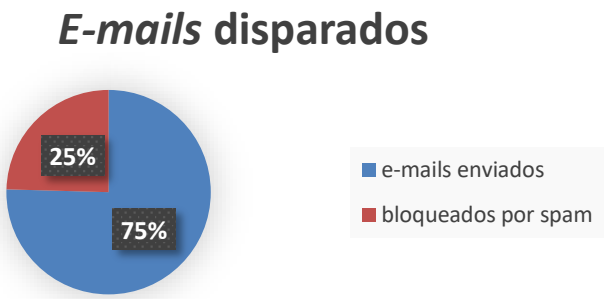
Com o Gophish instalado foram configurados os *e-mails* de remente, cadastro dos *e-mails* dos funcionários alvos, criação de páginas web falsas para captura de informações sensíveis, elaboração do conteúdo de *e-mail* com html e geração de *templates* para envio em massa, e coleta dos resultados gerada pela dashboard do próprio *framework*.

A criação dos *e-mails* contou com o auxílio dos profissionais de TI da Empresa Alpha com intuito de testar a fundo a capacidade de percepção dos colaboradores, utilizando-se endereço de *e-mail* semelhante ao da empresa, possíveis assuntos internos e senso de urgência.

4.4. Resultado dos testes de ataques *Phishing*

Os testes de Ataques de *phishing* foram realizados em dois dias da semana. Foram disparados 57 *e-mails* para os alvos utilizando-se de técnicas de engenharia social com objetivo de persuadi-los, 43 obtiveram sucesso no envio, 14 foram bloqueados por *spam*.

Figura 2 – Ataque de *phishing e-mails* disparados

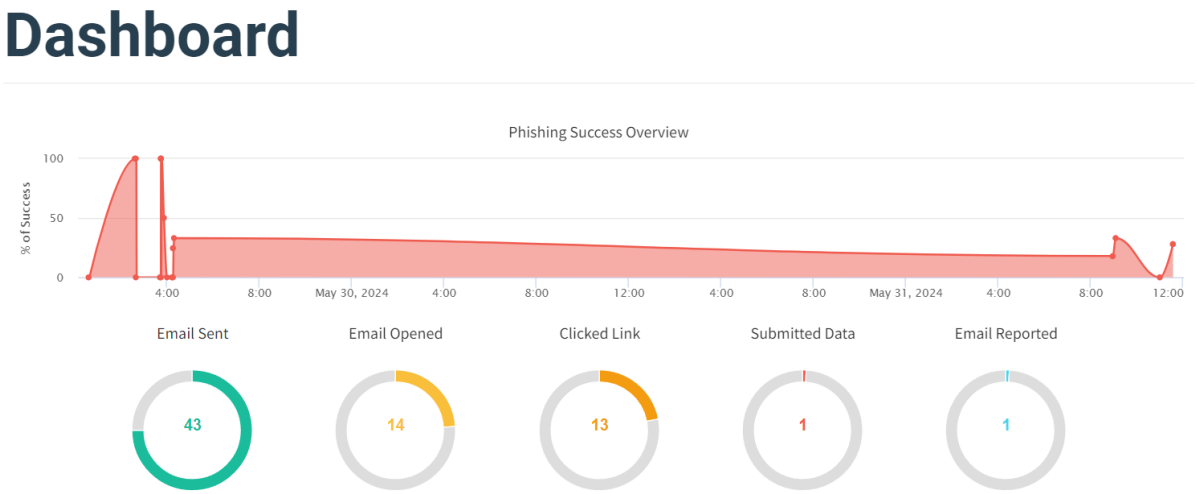


Fonte: Elaborado pelos autores, 2024

De 43 *e-mails* enviados, 14 deles foram abertos pelos alvos que foram induzidos a clicar em *links* falsos que os redirecionavam a uma *landing page* de *phishing* com a aparência de um *site* oficial, em 13 *e-mails* os usuários clicaram no *link* e a *landing page* foi aberta exibindo uma tela de login referente a plataforma de *e-mail* que a empresa utiliza, no intuito de capturar as credenciais de acesso.

Após esses disparos somente uma área reportou a equipe de TI da empresa sobre uma suspeita em relação aos ataques de *phishing*, como demonstra o *dashboard* abaixo.

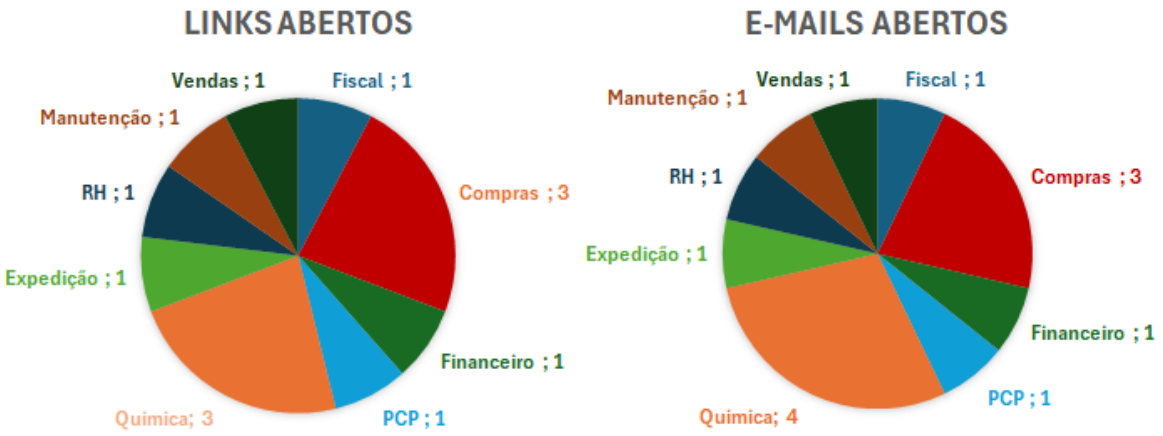
Figura 3 – Dashboard *framework* Gophish



Fonte: *Framework* Gophish, 2024

A única área que recebeu os *e-mails* e não abriu foi: Gestão Comercial. Apenas um único usuário do setor de Química submeteu suas credências de login e senha.

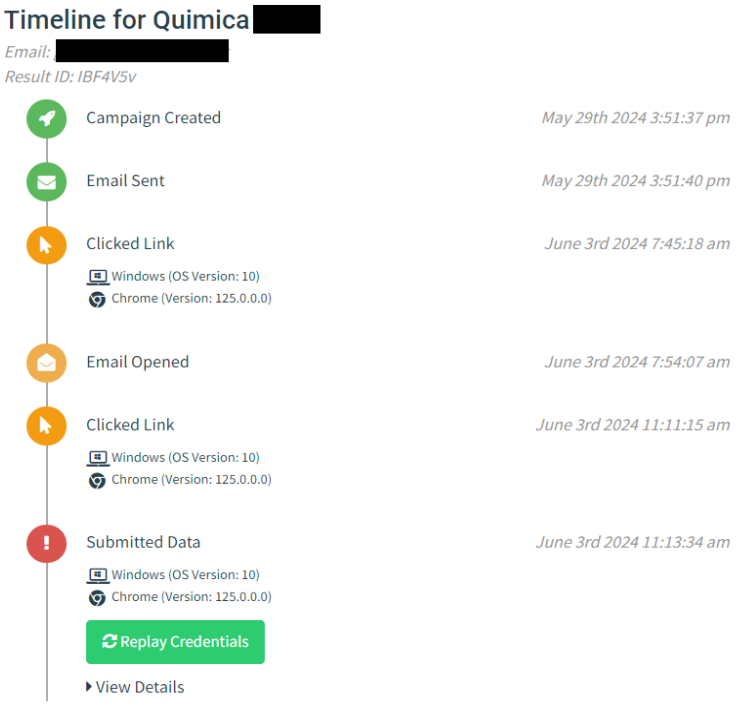
Figura 4 – *E-mails* e *links* abertos



Fonte: Elaborado pelos autores, 2024

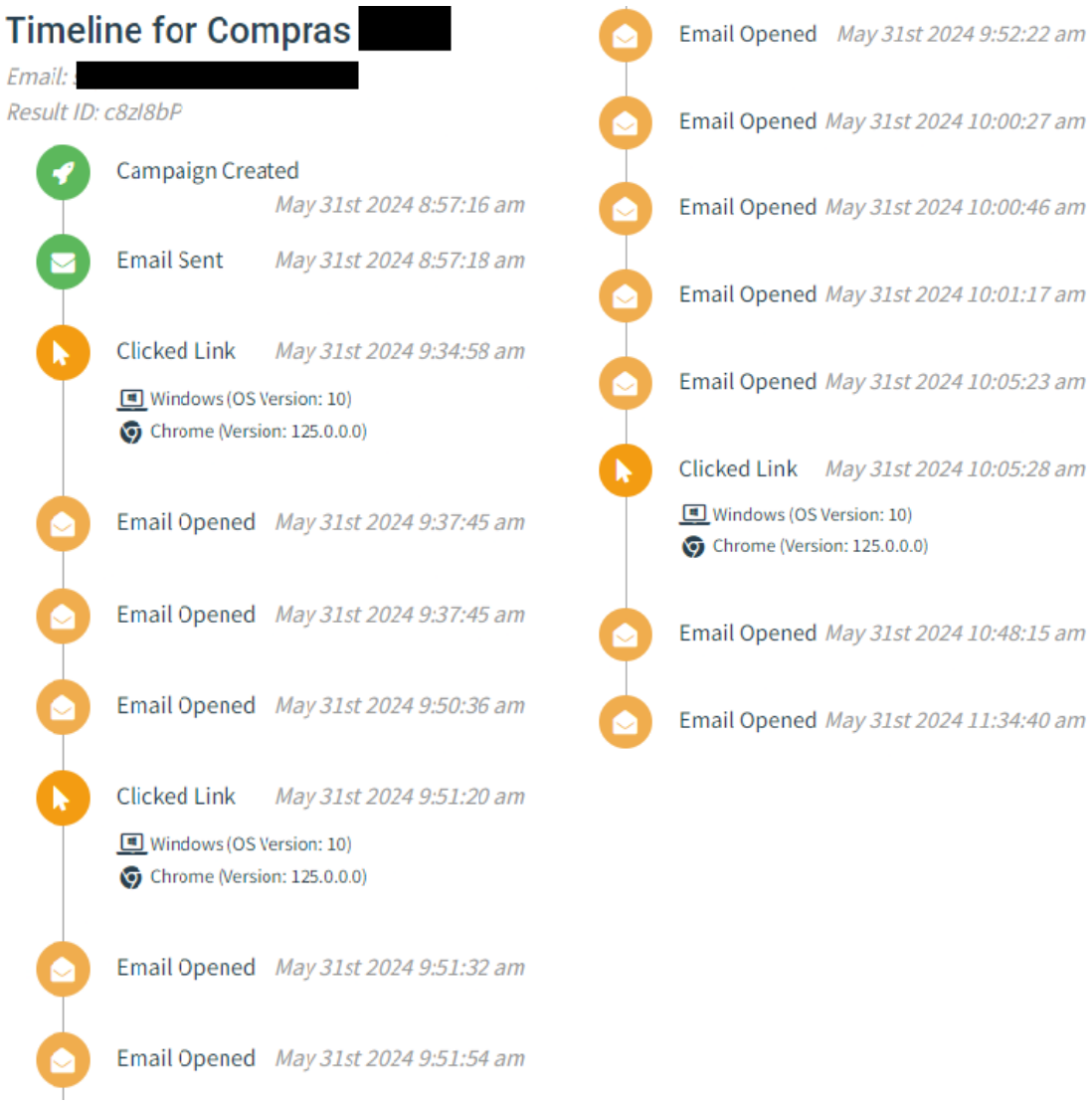
As demais apresentaram risco a empresa ao abrir e sucessivamente clicar nos *links* falsos que a redirecionavam a página de *phishing*. As áreas em que apresentaram maior vulnerabilidade foram a de Compras e Química que abriram 3 e 4 *e-mails* de *phishing* sucessivamente e clicaram no *link* falso, além disso a área de Química submeteu suas credenciais de acesso através da *landig page* falsa.

Figura 5 – *Timeline* de ação do usuário Química



Fonte: *Framework* Gophish, 2024

Figura 6 – *Timeline* de ação do usuário Compras



Fonte: *Framework* Gophish, 2024

Com esses dados conclui-se que a área de Química apresenta maior risco a empresa perante as demais, porém, também é possível ter ciência de que quase todas as áreas estiveram suscetíveis a ataques clicando no *link* malicioso, o que mostra que um treinamento sobre ataques de *phishing* pode ser necessário para toda a organização.

4.5 Análise dos Dados obtidos

Por meio do questionário, elaboração da arquitetura e testes de ataques phishing foi possível identificar vulnerabilidades que podem fazer com que a empresa esteja suscetível a ataques de phishing e em alguns casos sofrer danos que podem ser irreversíveis. A tabela abaixo mostra a relação das 10 vulnerabilidades identificadas a partir dos dados coletados:

Tabela 2 – Vulnerabilidades (VL) identificadas pela coleta de dados

Fonte	Questionário	Arquitetura	Ataques de *Phishing*
VL01	Negligência a *e-mails* internos e de clientes.	Não possui monitoramento de rede ativo.	Ineficiência dos filtros de *spam* utilizados.
VL02	Ausência de ferramentas para análise de *e-mails*.	A rede não é segmentada.	Inexistência de controle de *e-mails* que podem ser enviados (*whitelist*).
VL03	Ausência de antivírus especializados.	-	Menos de 10% dos *e-mails* abertos reportados para equipe de TI.
VL04	Ausência de treinamentos recorrentes.	-	Aproveitamento de 90% nos *e-mails* que utilizaram de engenharia social.

Fonte: Elaborado pelos autores, 2024

A tabela será utilizada para que seja criada a proposta de mitigação e sugestões de melhoria visando atacar todos os pontos de possíveis falhas identificados.

4.6 Propostas de mitigação dos ataques Phishing e Sugestões

A proposta visa apresentar a empresa um conjunto de práticas e medidas a serem adotadas para que a organização se torne menos vulnerável a ataques *phishing* além de minimizar os riscos e danos de um ataque bem-sucedido através de sugestões.

4.6.1 Educação e Treinamento

Com os dados coletados é perceptível a necessidade de treinamentos com o intuito de informar e atualizar os funcionários sobre as técnicas mais utilizadas por atacantes de *phishing*, essa prática seria capaz de tratar 4 vulnerabilidades identificadas, nos momentos do questionário (VL01 e VL04) e ataques *phishing* (VL03 e VL04).

O treinamento recorrente ajudaria aos usuários a identificarem: remetentes suspeitos, avaliar *links* e anexos, atentar-se mais a *e-mails* internos com o mesmo cuidado dado a externos, aumento de conscientização e senso crítico, conhecimento das técnicas mais utilizadas na engenharia social, além estarem condicionados a reportar a equipe de TI todos os *e-mails* em que identifiquem como suspeitos.

Essa prática poderia diminuir consideravelmente o número de *links* que foram clicados após os usuários terem aberto os *e-mails* de testes de ataque, aumentar o *report* a equipe de TI, inclusive de *e-mails* com assuntos internos, e nivelar o conhecimento de todos os funcionários para que todos tenham ciência dos impactos que a empresa pode ter caso um *phishing* seja bem-sucedido.

É de extrema importância de que todos os usuários tenham a consciência de que se os *links* clicados e dados submetidos fossem capturados por atacantes reais poderia gerar sérias consequências para a empresa podendo até ocasionar em grandes perdas financeiras.

4.6.2 Adoção de ferramentas de segurança

A adoção de algumas ferramentas de segurança também se faz necessária para que a empresa se torne menos vulnerável aos ataques. Como a principal ferramenta utilizada para envio de ataques *phishing* é o *e-mail*, utilizar-se de um *software* especializado na análise

pode ajudar a identificar o tráfego de *e-mails* suspeitos na rede.

Esse *software* combinado com um bom antivírus contratado pela empresa poderia aumentar o nível de segurança já que atividades suspeitas não identificadas pelo *software* de *e-mail* podem ser interceptadas e bloqueadas pelo antivírus, o que hoje não é possível já que a empresa utiliza da ferramenta de antivírus padrão do sistema operacional que se demonstra limitada em quesitos como: integridade da rede, atualizações inadequadas e falta de proteção contra endereços de *sites* maliciosos. A adoção dessas duas ferramentas seria capaz de eliminar duas vulnerabilidades identificadas no questionário respondido pela a Gerência de TI (VL02 e VL03).

Além dessas ferramentas é de extrema importância para a segurança e continuidade de negócios da organização a implementação de ferramentas de monitoramento de rede como IDS e IPS. Um IDS pode monitorar todo tráfego de rede em busca de atividades suspeitas ou maliciosas e alertar os administradores sobre possíveis ameaças, já o IPS pode ser capaz não só de detectar, mas também de bloquear as atividades maliciosas em tempo real, dessa forma, impedindo que cheguem aos sistemas finais. Elas também podem ser uteis pois analisam o histórico e padrões de tráfego, identificando anomalias que preveem tentativas de ataques de *phishing* com técnicas de camuflagem sofisticadas.

Outras vantagens da utilização do IDS e IPS são: visibilidade e relatórios, detecção proativa e reativa de ataques *phishing*, além de servir como uma camada adicional de defesa, adotando-se assim uma estratégia de segurança em profundidade na Arquitetura (VL01).

4.6.3 Adequação de arquitetura

Uma vulnerabilidade que foi identificada na arquitetura (VL02) que pode fazer com que um ataque bem-sucedido de *phishing* coloque em risco a operação de toda organização é que a rede não foi segmentada, isso quer dizer que uma falha pode ocasionar no comprometimento de toda a rede e consequentemente paralisar toda a operação e em alguns casos por tempo indeterminado.

A adoção de Virtual Local Area Networks (VLANs) na arquitetura da rede pode ajudar a segmentar já que adicionando-a é possível dividir a rede entre setores e assim que uma das máquinas for contaminada por um vírus através de um *phishing* seriam afetados somente os outros dispositivos que estão na mesma VLAN, dessa forma evitando a inatividade de toda empresa.

Além dessa adequação é recomendável que seja criada uma redundância de rede, que se refere a implementação de caminhos alternativos de comunicação e a duplicidade de componentes da infraestrutura para garantir a continuidade do serviço em caso de falhas ou invasões.

Com a redundância é possível isolar a área da rede comprometida sem que ela fique indisponível já que é possível transferir as operações da área para outro dispositivo redundante enquanto a equipe de TI trabalha para recuperar o ambiente corrompido, identificar a origem do ataque e bloquear possíveis novas tentativas de ataques.

4.6.4 Configurações de segurança relacionadas a e-mail

A implementação de uma *whitelist* para controle de *e-mails* auxilia a especificar quais endereços de *e-mails* são permitidos, garante uma comunicação mais segura, reduzindo drasticamente o risco de ataques de *phishing* (VL02) e *spam*. A *whitelist* também facilita a conformidade com políticas de segurança permitindo um controle rigoroso sobre quem pode enviar *e-mails* à organização, criar e manter uma *whitelist* também aprimora a eficiência e a confiabilidade das comunicações por *e-mail*.

A reconfiguração dos filtros de *spam* é uma medida essencial para garantir a integridade e a eficiência das comunicações por *e-mail*. Com filtros inadequados, há um aumento no risco de que mensagens indesejadas ou maliciosas cheguem às caixas de entrada, comprometendo a segurança dos dados. Ao reconfigurar esses filtros, ajustando os parâmetros e critérios de detecção, é possível reduzir significativamente a quantidade de ataques de *phishing* (VL01) e *spam* recebido, permitindo uma filtragem mais precisa, assegurando que apenas *e-mails* legítimos e relevantes sejam entregues, o que contribui para uma experiência de comunicação mais limpa e segura para todos os usuários.

5. Conclusões

Foi possível identificar que a utilização de ferramentas de segurança, antivírus e controle de *e-mails* é uma forma de mitigar os ataques de *phisihng,* mas não indica ser a forma completa. A aplicação de treinamentos para a uma educação dos colaboradores na análise de *phishing* corrobora para a solução.

A organização demonstrou algumas inconsistências relacionadas a este método de ataque que poderia ter colocado em risco toda a operação da organização na hipótese de uma tentativa real.

É perceptível com base nos resultados, que além da ausência de ferramentas de segurança os atacantes se beneficiam com a fragilidade humana e desinformação para obter sucesso nos ataques.

Apesar do sucesso no teste para captura de credenciais de login e senha o simples click no *link* falso era o suficiente para executar a instalação de um *software* malicioso na rede o que deixou claro a necessidade de implementação e recorrência de treinamentos para a introdução e conscientização aos ataques de *phishing*.

Também se demonstraram necessárias à implementação de ferramentas para interceptação e contenção de ataques, assim como a apropriação da arquitetura aderindo tecnologias ou componentes que permitam a disponibilidade dos sistemas e operações mesmo que um ataque adentre a rede.

A contribuição para a prática é a de que o gestor de TI da Empresa-Alpha assim como outros gestores que se enquadram em um contexto semelhante possam tirar proveito da proposta e sugestões desta pesquisa com objetivo de mitigar ataques de *phishing* em uma empresa do ramo automotivo. A contribuição para a academia é acrescentar em pesquisas futuras que envolvam ataques de *phishing* e suas formas de contenção.

Referências

ALKHALIL, Z. et al. Phishing attacks: A recent comprehensive study and a new anatomy. **Frontiers in Computer Science**, v. 3, p. 563060, 2021.

CASOTTI, B.; GOLDENSTEIN, M. Panorama do setor automotivo: as mudanças estruturais da indústria e as perspectivas para o Brasil. [s.l: s.n.]. Disponível em: <https://web.bndes.gov.br/bib/jspui/bitstream/1408/2566/1/BS%2028%20Panorama%20do%20setor%20automotivo_P.pdf>.

DAVIES, N. The top 8 Cybersecurity threats facing the automotive industry heading into 2023. Disponível em: <https://cybersecurity.att.com/blogs/security-essentials/the-top-8-cybersecurity-threats-facing-the-automotive-industry-heading-into-2023>.

DIAS, P. R. S. Prevenir um Ataque de Phishing. PhD Thesis—[s.l: s.n.]. Disponível em: <https://comum.rcaap.pt/handle/10400.26/39283>

FONSECA, M. Engenharia social: conscientizando o elo mais fraco da segurança da informação. 1 jan. 2017.

FONTES, E. L. G. SEGURANÇA DA INFORMAÇÃO. [s.l.] Saraiva Educação S.A., 2017.

FREUND, G. P. et al. Mecanismos tecnológicos de segurança da informação no tratamento da veracidade dos dados em ambientes Big Data. Perspectivas em Ciência da Informação, v. 24, p. 124–142, 2019.

GONÇALVES, G. V. C.; OGAWA, K. R. L.; LIMA, M. A. DE. Engenharia social e a segurança da informação. 2022.

KASPERSKY. O que é o DNS? Brasil: Kaspersky, 2024. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/dns>.

LIMA, M. D. A. Segurança da informação na pandemia de covid-19 no brasil: a cibereducação como medida preventiva contra ataques de phishing. 2022.

MASOUMI, S. M.; KAZEMI, N.; ABDUL-RASHID, S. H. Sustainable supply chain management in the automotive industry: A process-oriented review. Sustainability, v. 11, n. 14, p. 3945, 2019.

MOHAMED, A. K. Y. S. et al. A systematic literature review for authorization and access control: definitions, strategies and models. International Journal of Web Information Systems, v. 18, n. 2/3, p. 156–180, 2022.

OLIVEIRA TEODORO, T.; CISA, C. Managing Technology Risk to Protect Privacy and Confidentiality. 2020.

PEREIRA, N. DE L. B.; NEVES, L. M. Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus). Revista Tecnológica da Fatec Americana, v. 9, n. 01, p. 68–83, 2021.

SILVA, B. E. L. Serviços de segurança em computação em nuvem usando a plataforma amazon web service (AWS). 2023.

SOUZA, F. B. USUÁRIO, O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO. Revista Scientia Alpha, v. 3, n. 03, 2022. Disponível em: <https://revista.alfaumuarama.edu.br/index.php/rsa/article/view/34/33>.

VERIZON. DBIR 2020 Data Breach Investigations Report. EUA: Verizon, 2020. Disponível em: <https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report>.

VERIZON. DBIR 2023 Data Breach Investigations Report. EUA: Verizon, 2023. Disponível em: <https://www.verizon.com/business/resources/T4c4/reports/2023-data-breach-investigations-report-dbir.pdf>.

YIN, R. K. Estudo de Caso: Planejamento e Métodos. 5. ed. São Paulo: Bookman, 2014.

APENDICE A – Questionário

Conteúdo: Prevenção

#	**Pergunta**
Q1	Quais medidas proativas são implementadas para educar os funcionários sobre os riscos do *phishing*?
Q2	Como incentivar uma cultura de segurança cibernética em toda a organização, onde todos os funcionários se sintam responsáveis pela prevenção de ataques de *phishing*?
Q3	Quais são os riscos específicos de *phishing* associados a fornecedores e parceiros externos e como podem mitigá-los?
Q4	Como é possível implementar treinamentos regulares de conscientização sobre segurança cibernética para garantir que os funcionários estejam atualizados sobre as últimas táticas de *phishing*?

Conteúdo: Contramedidas

#	**Pergunta**
Q5	Quais tecnologias de segurança adicionais são adotadas para detectar e bloquear melhor os ataques de *phishing*?
Q6	Como a empresa pode fortalecer a política de segurança de *e-mail* para filtrar e identificar melhor *e-mails* de *phishing*?
Q7	Quais são as melhores práticas para verificar a autenticidade de *e-mails* suspeitos antes de clicar em *links* ou fornecer informações confidenciais?
Q8	Como implementar políticas de acesso e permissões que limitem o acesso a informações confidenciais, mesmo em caso de comprometimento de credenciais?

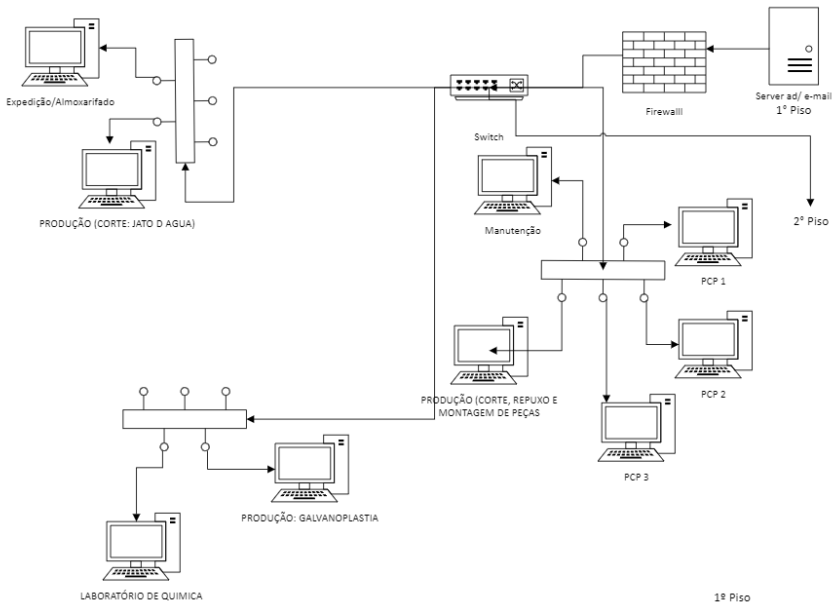
Conteúdo: Medidas Proativas e Reativas

#	**Pergunta**
Q9	Quais são os sinais de alerta precoce que devem estar atentos para identificar possíveis ataques de *phishing* direcionadas à empresa?
Q10	Como vocês avaliam regularmente a eficácia das medidas de mitigação de *phishing* e fazer ajustes conforme necessário?

APENDICE B – Arquitetura de TI da empresa

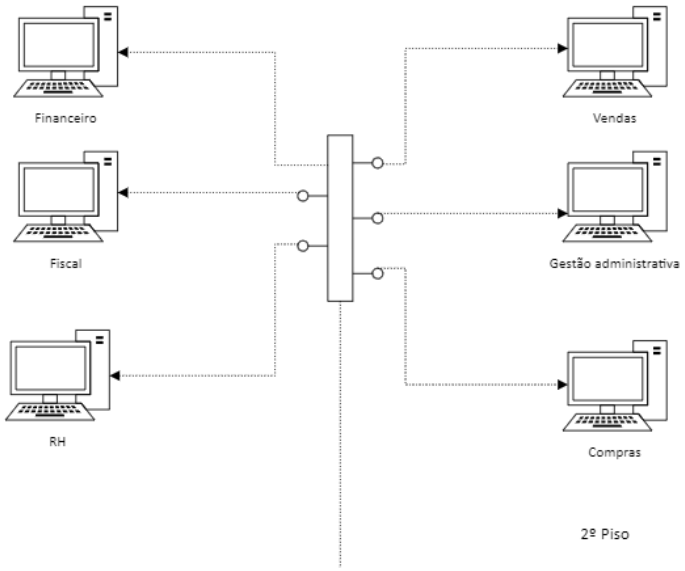
O desenho das arquiteturas foi confeccionado e aprovado junto a equipe de TI da Empresa-Alpha assim como nos desenhos abaixo:

Figura 7 – Arquitetura de TI do Piso 1



Fonte: Elaborado pelos autores, 2024

Figura 8 – Arquitetura de TI do Piso 2



Fonte: Elaborado pelos autores, 2024

Expedição/Almoxarifado: É a área responsável pelo recebimento de matéria prima e pela preparação para o envio de peças já fabricadas e faturadas.

Produção: Operadores de máquinas e auxiliares de produção. Atuam em operações como solda, corte, repuxo e manuseio de máquina de produção para fabricação de peças. Somente dois colaboradores possuem acesso a computadores ligados a rede somente para apontamento de ordens de produção e consulta de desenhos no sistema da empresa.

Manutenção: Área responsável pela manutenção das máquinas de produção e conserto de equipamentos utilizados no dia a dia da empresa.

PCP (Planejamento e Controle de Produção): Criam planos de controle para produção de peças, desenhos detalhados de fabricação, acompanham e auxiliam nos processos de desenvolvimento e produção de peças.

Laboratório de Química: Responsáveis por acompanhar o banho químico de peças no setor de Galvanoplastia, desenvolver novas fórmulas e melhorias no setor.

Galvanoplastia: Operadores responsáveis pelo banho químico das peças com prata e cobre.

RH (Recursos Humanos): Gerencia o ciclo de vida dos funcionários. Contratam, recrutam, treinam, integram e demitem funcionários, além de administrar seus benefícios.

Financeiro: Administram todo o balanço financeiro da empresa. Toda entrada e saída de capital

Fiscal: Responsável pela emissão de notas e faturamento de pedidos

Vendas: Se relaciona com clientes fechando contratos e novas solicitações de pedidos para fabricação de peças

Gestão administrativa: Essa área tem um conhecimento geral do funcionamento de todas as outras áreas que compõem a empresa e sempre está analisando seus relacionamentos e resultados em busca de melhorias para que todos os departamentos funcionem bem em conjunto

Compras: Esse setor está ligado a cadeia de suprimentos da empresa e está sempre sendo requisitado para conseguir os melhores preços e fornecedores de materiais e recursos que são necessários para produção de peças e funcionamento da empresa.